|  |  |
| --- | --- |
| **How to hide your WordPress plugins** Why do you need to hide all plugin-related info? For example, there was a bug in one of your plugins, say, in a version 1.4.5, and that has caused vulnerability problems. Hacker knows about this bug, which means, that he is positive that if you have a fictional plugin version 1.4.5 then your website can be hacked easily.  How can a hacker identify plugin’s name and the version?  All WordPress plugins are stored in the **/wp-content/plugins** directory. And if you look at the frontend of the HTML code, you’ll see how plugins add up their resources exposing themselves in the process:  Как скрыть информацию о плагинах WordPress?  Just a quick glance at the URL below tells us that the plugin **elementor** has been installed on **the blog:**     1. https://-domain-name-/wp-content/plugins/elementor/assets/lib/jquery-numerator/jquery-numerator.min.js   And there is no difficulty in finding out its version:   1. https://-domain-name-/wp-content/plugins/elementor/readme.txt  **How to hide plugin-related info** We’ll need the [Clearfy](https://clearfy.pro/) plugin with its active component named [Hidemywp](httsp://clearfy.pro/hide-my-wp/)**.**  Open the Clearfy menu, go to the “Protection” and switch to the “Main directories Confidentiality” tab. Select “**Change path to the plugins directory”**. This section helps to hide your plugins and its content from hackers.  Как скрыть информацию о плагинах WordPress?  Now we need to set up these features properly. **New path to the plugins directory** **Enter a new path to the plugins directory using letters and numbers only. Escape slashes before and after the line. For example, if you enter the word “modules”, then the path to the elementor plugin will look like this:** [**http://-domain-name-/modules/elementor/**](http://-domain-name-/modules/elementor/)  Note: this setting doesn’t change the actual directory names. Disable the plugin to undo the change. **Rename plugins** This feature replaces plugin names with a random set of characters – **79f6d4d2.**  **If the path to the elementor plugin looked this way** <http://-domain-name-/modules/elementor/>, then now it will be replaced by this: <http://-domain-name-/modules/79f6d4d2/>.  This feature gives you two options: you can rename either all plugins or only active ones. But do you really need to rename inactive plugins? The point is that even if the plugin has been deactivated, its content is still accessible to anyone. Inactive plugins can’t be hacked unless there are severe violations of coding standards. If your priority is the speed optimization of the website, then choose “Only active”. However, if you want to hide all traces of using WordPress, then you’ll need the “All plugins” option. **Block access to the directory** Whenever you change the path to the plugins directory, it is still accessible through the link. This feature blocks user access to the <http://-domain-name-/wp-content/plugins/elementor/readme.txt> address. Now whenever a user tries opening this page, he’ll get 404 error of the theme. **Hide the readme.txt file** We’ve changed the path to the plugins directory and hid all plugin names. But if we follow the link:   1. https://-domain-name-/modules/79f6d4d2/readme.txt   we’ll see the content of the readme.txt file, where plugin name and versions are located. That’s why you need to block access to this file for all users.  Open the Clearfy menu, go to the “**Protection**” and switch to the “**Main settings**” tab. Select “**Files & Directories”.**  Как скрыть информацию о плагинах WordPress?  Enable the “Hide service files (.txt,.log,.html)” feature, as it will block access to all service files with information about your website.  ПРИМЕЧАНИЕ: Надо проверить названия вкладок Protection или Security и т.д. Как бы это делать сразу при получении текста? + В переводе интерфейса плагина есть ошибки…. | **Как скрыть информацию о плагинах WordPress?** Для чего нужно скрывать информацию о ваших плагинах? В одном из ваших плагинов версии 1.4.5, разработчики допустили ошибку, из-за чего плагин стал уязвим. Злоумышленник знает об этой уязвимости, а значит он уверен, что если у вас установлен выдуманный нами плагин версии 1.4.5, то ваш сайт можно легко взломать. Как злоумышленник может узнать версию и имя плагина? В WordPress все плагины хранятся в директории **/wp-content/plugins**. Если посмотреть в html код страницы с фронтальной стороны сайта, мы сможем увидеть, как плагины подключают свои ресурсы, тем самым выдавая себя:  Как скрыть информацию о плагинах WordPress?  Просто посмотрев на URL ниже, мы явно сможем определить, что на блоге установлен плагин **elementor**   1. https://-domain-name-/wp-content/plugins/elementor/assets/lib/jquery-numerator/jquery-numerator.min.js   Теперь мы легко сможем узнать версию плагина:   1. https://-domain-name-/wp-content/plugins/elementor/readme.txt  Скрываем информацию о плагинах Для выполнения этой задачи нам понадобится плагин [Clearfy](https://clearfy.pro/) и его активный компонент [Hide my wp](httsp://clearfy.pro/hide-my-wp/)**.**  В плагине Clearfy перейдите в раздел “**Защита**” и нажмите на закладку “**Конфиденциальность основных директорий**” и найдите раздел “**Изменить путь к директории plugins**“. Этот раздел настроек помогает скрыть ваши плагины и их содержимое от злоумышленников.  Как скрыть информацию о плагинах WordPress?  Теперь нам нужно правильно настроить эту группу опций. **Новый путь к директории plugins** Введите новый путь к вашей директории plugins, используя только буквенно-цифровые символы без слешей в начале и конце строки. Пример: если вы введете слово “modules”, ваш путь к плагину elementor будет выглядеть вот так http://-domain-name-/modules/elementor/  Примечание: эта настройка не меняет фактические имена директорий, при отключении плагина эффект плагина исчезнет без последствий. **Переименовать плагины** Эта настройка подменяет имена плагинов случайным набором символов **79f6d4d2**.  Если путь к плагину elementor выглядел вот так http://-domain-name-/modules/elementor/, теперь он будет выглядеть так http://-domain-name-/modules/79f6d4d2/.  Есть два варианта этой настройки, переименование только активных плагинов и всех. Нужно ли переименовывать неактивные плагины? Дело в том, что даже если плагин деактивирован, любой может получить доступ к его содержимому. Неактивные плагины не подвержены взлому, если только в них нет серьезных нарушений стандартов кодирования. Если вы заботитесь об оптимизации скорости сайта, вам подойдет вариант “Только активные”, но если вы хотите максимально скрыть признаки использования WordPress, вам стоит выбирать “Все плагины”. **Заблокировать доступ к директории** После того, как вы изменили путь к директории plugins, доступ по ссылке к директории по-прежнему открыт. Эта опция позволяет заблокировать пользовательский доступ по URL http://-domain-name-/wp-content/plugins/elementor/readme.txt, теперь если пользователь попробует запросить эту страницу, он получит 404 ошибку вашей темы по умолчанию. **Скрываем файл readme.txt** Мы подменили путь к директории плагинов и скрыли названия плагинов. Но если мы перейдем по ссылке:   1. https://-domain-name-/modules/79f6d4d2/readme.txt   У нас откроется файл readme.txt, где можно увидеть название плагина и его версию. Поэтому для нас важно закрыть доступ к этому файлу для всех пользователей.  В плагине Clearfy перейдите в раздел “**Защита**” и нажмите на закладку “**Основные настройки**” и найдите раздел “**Файлы и директории**“.  Как скрыть информацию о плагинах WordPress?  Включите опцию “Скрыть сервисные файлы (.txt,.log,.html)”, эта опция заблокирует доступ ко всем сервисным файлам, которые содержат информацию о вашем сайте. |